

Case Report

National Gallery DC

Tracy's iPhone [2012-07-15-National-Gallery]

Table of Contents

[Case Report](#)

[National Gallery DC](#)

[Tracy's iPhone \[2012-07-15-National-Gallery\]](#)

[Table of Contents](#)

[Executive Summary](#)

[Equipment and Tools](#)

[Details of Tracy's iPhone](#)

[Evidence to Establish Personas](#)

[Evidence relating to theft of valuable stamps](#)

[Evidence relating to defacement of museum art](#)

[Plot Timeline](#)

[Conclusion](#)

[Appendix A: Correspondence Evidence](#)

[Appendix B: WiFi and GPS Location Information](#)

Executive Summary

On January 21, 2016, Digitech Inc. was called in to assist the National Gallery, Washington D.C. (NGDC) case involving the conspiracy associated with the theft of valuable stamps and defacing of museums are at the NGDC.

- Tracy is a suspect in the aforementioned conspiracy.
- As part of the investigation, Tracy's iPhone was taken into custody.
- Digitech, Inc. was tasked with investigating evidence relevant to the aforementioned conspiracy.

As described fully in the report, Digitech, Inc. made the following findings.

A plot in the making was shown to be planned as evidence shows from Tracy's phone with her accomplices Pat, Carry, and King. Tracy, Pat, and King have set a plan to steal stamps from the NGDC while Tracy uses the information to assist her acquaintance Carry with a flash-mob which is a cover-up to deface and damage artwork at the NGDC.

Equipment and Tools

The tools and equipment used to gather and analyze the evidence gathered:

Kali Linux [operating system]

Autopsy [forensics tool]

DB Browser for SQLite [database]

Nano [text editor]

Google Earth/Maps [gps/location]

Details of Tracy's iPhone

Case Name: 2012-07-15-National-Gallery

Case #: 1EZ215-P

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone 1, 2	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtwelve's iPhone	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/logs/lockdownd.log

OS Version	iPhone OS 4.2.1 (8C148)	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log
Install Time	6/6/2012 12:03:28 -0700	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log
User Email	tracysumtwelve@gmail.com	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Mail/Protected Index
Phone Number	1 (703) 340-9661	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/logs/lockdownd.log
Serial Number	86004482Y7H	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log
ICCID	89014103255195342366	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/logs/lockdownd.log
IMEI	012021003735398	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/root/Library/Lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	

Evidence to Establish Personas

This section establishes aliases, phone numbers, emails addresses associated with each person, and relationships between each individual.

Tracy:

Phone Number: (703) 340-9961
 Personal Email: tracysumtwelve@gmail.com
 Work Email: tracy.sumtwelve@nationalgallerydc.org
 Alt Email: coralblue@hotmail.com
 Relationship: Accused

Pat:

Phone Number: (571) 308-3236
Email: patsumtwelve@gmail.com
Alt Email: perrypatsum@yahoo.com
Relationship: Brother (Alias is Perry) / Accomplice

Terry:

Phone Number: (703) 829-6071
Relationship: Daughter of Tracy and Joe

Joe:

Email: joe.sum.twelve@gmail.com
Relationship: Ex-Husband, Father of Terry

Carry:

Phone Number: (202)725-2124
Email: carrysum2012@yahoo.com
Relationship: Acquaintance

King:

Email: throne1966@hotmail.com
Relationship: Acquaintance of Pat

- *Pat and Carry are accomplices to Terry's plans and have included a third party member by the name of King who will assist the three in the robbery.*
- *Terry is the daughter of Terry and Joe, Joe being the ex-husband of Terry.*
- *Pat is Terry's brother.*

Evidence relating to theft of valuable stamps

This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps.

Evidence collected shows that Tracy, Pat, and King worked with one another in order to steal valuable stamps from the NGDC. Emails and SMS messages provide information about plotted plans to steal these valuables.

Pat had reached out to King through email in order to ask for his assistance in the heist to the NGDC (Appendix A #8, #10).

King had agreed to assist with the heist by providing an attachment titled 'needs.txt' which contained information on the equipment list he would use on this plan (Appendix A #10)

Pat has then reached out to his sister Tracy through SMS to change attachment files to a pdf format to a 'friend' who was also Tracy under a different alias (Appendix A #27)

The pdf files that were then changed were compressed into a ZIP file titled 'documents.zip' that contain three pdf files under the name 'Stamp insurance' that Tracy had sent to her alias coralbluetwo@hotmail.com (Appendix A #9)

Evidence relating to defacement of museum art

This sub-section provides details regarding the evidence found as it relates to the defacement of museum art.

The collection of evidence shows that Tracy works alongside her acquaintance Carry in order to carry out a 'flash-mob' guise defacement of the NGDC gallery.

With collections of email and SMS, text messages detail an exchange with Tracy and Carry planning to meet up for lunch to speak more of their plan at Bubba's Grill (Appendix A #11, #19)

Email exchanges indicate a thread where Carry suggests lunch as well as inquiring on ways to get her tablet into the gallery in order to get pictures for her flash-mob event and carries out a plan to meet up the following day around 9 with the tablet (Appendix A #11)

Text message exchanges show a meetup on the day of where Carry is on her way to the NGDC and for her to carry the tablet inside so Tracy could have it and assist her in the planned 'flash-mob' (Appendix A #32, #33, #34)

Plot Timeline

[Tuesday. June 19, 2012]

- Pat provides instructions on setting up a Virtual Machine under the guise of a 'mp3' song to Tracy.

[Thursday. July 05, 2012]

- Carry asks Tracy about getting together and meeting up for lunch at Bubba's Grill.

[Friday. July 06, 2012]

- Carry and Tracy meet up at Bubba's Grill as stated in text messages.
- Pat gives Tracy credentials for an alias email they should use in which Pat, Tracy, and another accomplice by the name of King begin planning.

[Monday. July 09, 2012]

- Tracy sends herself at her alias email attachments containing information about Stamp insurance.

[Tuesday. July 10, 2012]

- King sends documents about the equipment he needs to use in the heist.
- Carry asks Tracy about how to get her tablet into the gallery and if Tracy could help with it before asking if she can come the next day around 9.

[Wednesday. July 11, 2012]

- Carry meets up with Tracy and gives the tablet to Tracy to take into the NGDC.

Conclusion

Evidence found on Tracy's iPhone indicated the following:

Tracy -under the alias Coral- and her brother Pat -using the alias Perry- communicated with each other using alternate emails (Tracy: coralblue@hotmail.com/Pat: perrypatsum@yahoo.com) about their heist plans on the valuable stamps of the NGDC.

They had included another accomplice by the name of King through email in which King discusses the type of equipment he needs through a list they send as an attachment through email for him to use with the heist plan of the NGDC goods.

All while this is being planned out by Pat, Tracy, and King; Tracy is planning on the side to assist her acquaintance Carry with defacement of the gallery art at the NGDC under the guise of a 'flash-mob' that Carry plans as long as she is able to smuggle her tablet and any other electronics into the building with Tracy's help as discussed not only through email but through SMS.

Appendix A: Correspondence Evidence

This subsection will provide an amalgamation of the email and SMS correspondence evidence.

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
1	06/19/12 14:38:59	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Crazydave by the VMs	Pat emails Coral about just receiving the email sent to him and speaks of a new song by the “VMs” and what Coral thinks of them.	Mailbox Data Structure
2	06/19/12 13:26:48	F: perrypatsum@yahoo.com T: tracysumtwelve@gmail.com Subject: Look me up sometime	Pat under the alias ‘Perry’ asks Tracy to use an alias and talk to him through it in email.	Mailbox Data Structure
3	06/19/12 16:06:33	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Paris Speak and answer	Translated from french–Pat emails Tracy to let her know that he considers the proposal she has made and that they should speak to one another through an alias under another email address where further instructions will be provided.	Mailbox Data Structure
4	06/29/12 07:31:36	F: perrypatsum@yahoo.com T: tracysumtwelve@gmail.com Subject: hey sis	Pat has emailed Tracy but addresses her as ‘sis’ and asks about Tracy’s daughter Terry and wishing to keep in touch or check in often and to eat dinner as friends as he has been busy trying to sort stuff with Tracy’s friend Coral.	Mailbox Data Structure
5	07/02/12 12:34:46	F: engod.rikal@m57.biz T: tracysumtwelve@gmail.com Subject: Weekend plans	Engod tells Tracy that Avery and them are going to the park on the weekend to hangout and if Tracy would want to join for some frisbee.	Mailbox Data Structure
6	07/03/12 09:29:37	F: joe.sum.twelve@gmail.com T: tracysumtwelve@gmail.com	Original thread starting with Tracy asking Joe to help pay for Terry’s tuition.	Mailbox Data Structure

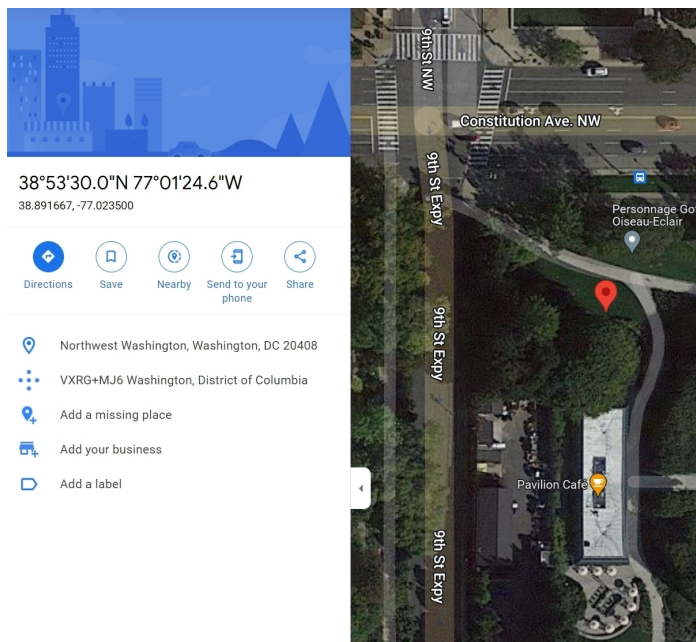
		Subject: Re: Regarding Terry	Joe responds with an apology and letting Tracy know that he will not help pay for Terry's tuition if she is not living with him.	
7	07/05/12 08:51:31	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Long time no see...	Carry speaks of seeing Tracy on facebook having a hard time and that they should get together and have lunch on Friday.	Mailbox Data Structure
8	07/06/12 11:27:51	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Good News	Original thread starting with Tracy letting Pat know that she had spoken with Coral about great news of her job and to catch up with her. Pat lets Tracy know of someone to help named 'king' and information about another account with login info: coralblue@hotmail.com PW: legalBee	Mailbox Data Structure
9	07/09/12 07:47:53	F: tracysumtwelve@gmail.com T: coralbluetwo@hotmail.com Subject: things	Contains attachments of a documents.zip folder containing 3 "Stamp insurance" pdf folder documents. The docs.zip attachment contains 3 "Stamp insurance" pdf files.	Mailbox Data Structure
10	07/10/12 15:24:58	F: patsumtwelve@gmail.com T: coralbluetwo@hotmail.com Subject: Fwd: can't pass up Attachment: needs.txt	King agrees to help with the heist and sends a document with a listing of equipment in preparation for it as saved as an attachment "needs.txt".	Mailbox Data Structure
11	07/10/12 06:48:40	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see	Original thread beginning with Tracy thanking Carry for lunch and that they should do lunch more often. Carry responds by inquiring on how to get her tablet into the gallery. The security isnt tight in the gallery and she wants to know if Tracy could pull some strings for her to get it in. Carry speaks of	Mailbox Data Structure

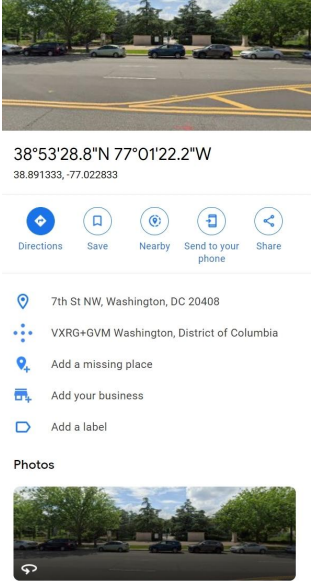
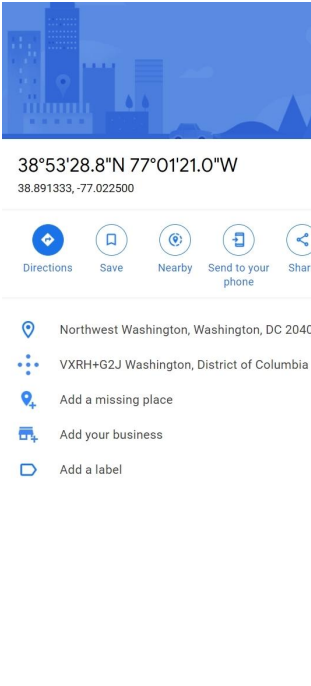
			<p>wanting to get pictures for her flash mob event she had spoken to Tracy about.</p> <p>Tracy responds in which she is able to get Carry's tablet in and when Carry would like to get in and take a look around the gallery.</p> <p>Carry asks if she can come tomorrow around 9. Tracy agrees and the plan is set to meet the next day around 9.</p> <p>Carry then asks about making the event they are putting together as painless as possible and if there is a way to change the shift of times and that she has a good budget for the event if Tracy would like information on it.</p>	
12	07/11/12 04:18:33	<p>F: microsoft@reply.digitalriver.com T: coralbluetwo@hotmail.com</p> <p>Subject: Only 30 days left! Start a free Office training course now.</p>	Spam/subscription email from "Microsoft Office"	Mailbox Data Structure
13		F: Pat T: Tracy	Pat asks Tracy what she is up to for the weekend.	SMS Messages
14		F: Terry T: Tracy	Terry tells Tracy that she will be going out with Joe after school for pizza.	SMS Messages
15		F: Tracy T: Pat	Tracy has no plans, asks Pat the same question of 'How about you?'	SMS Messages
16		F: Tracy T: Terry	Ok, sounds good.	SMS Messages
17		F: Tracy T: Terry	Tracy tells Terry they can't afford Prufrock anymore and if they could switch to someplace else.	SMS Messages

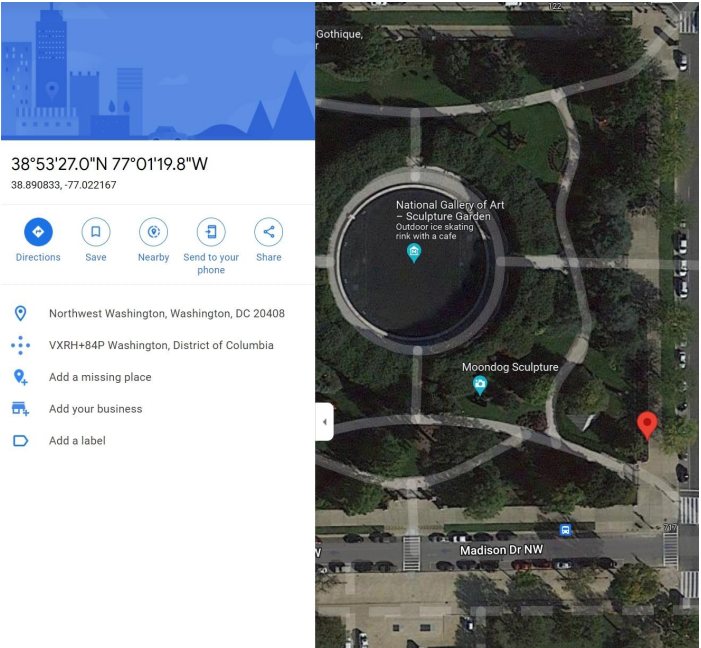
18		F: Terry T: Tracy	Terry lets Tracy know that it would be the worst and that living with Joe to be able to stay at prufrock would be a better option than switching schools.	SMS Messages
19		F: Carry T: Tracy	Meetup with Tracy at Bubba's grill at 1.	SMS Messages
20		F: Tracy T: Carry	Okay that sounds great. See you there	SMS Messages
21		F: Tracy T: Pat	Hey can you give me a call	SMS Messages
22		F: Pat T: Tracy	Pat is too busy to call, asks about doing it later.	SMS Messages
23		F: Tracy T: Pat	Tracy says that it is important and that Pat needs to call her back soon.	SMS Messages
24		F: Pat T: Tracy	Pat will call Tracy back in 5 minutes.	SMS Messages
25		F: Carry T: Tracy	Carry has a table at Bubba's grill ready.	SMS Messages
26		F: Tracy T: Carry	Tracy responds and says she will be right there 'brt'.	SMS Messages
27		F: Pat T: Tracy	Pat tells Tracy about 'Coral' having an email with an attachment that needs to be changed to a pdf file format.	SMS Messages
28		F: Tracy T: Pat	Tracy acknowledges Pat's message and will get on it.	SMS Messages
29		F: Terry T: Tracy	Terry asks Tracy if she would like to go to lunch with her.	SMS Messages
30		F: Tracy T: Terry	Tracy responds with being back at work.	SMS Messages
31		F: Terry T: Tracy	Terry tells Tracy that she is busy and that the weekend should be better if Joe isn't busy.	SMS Messages

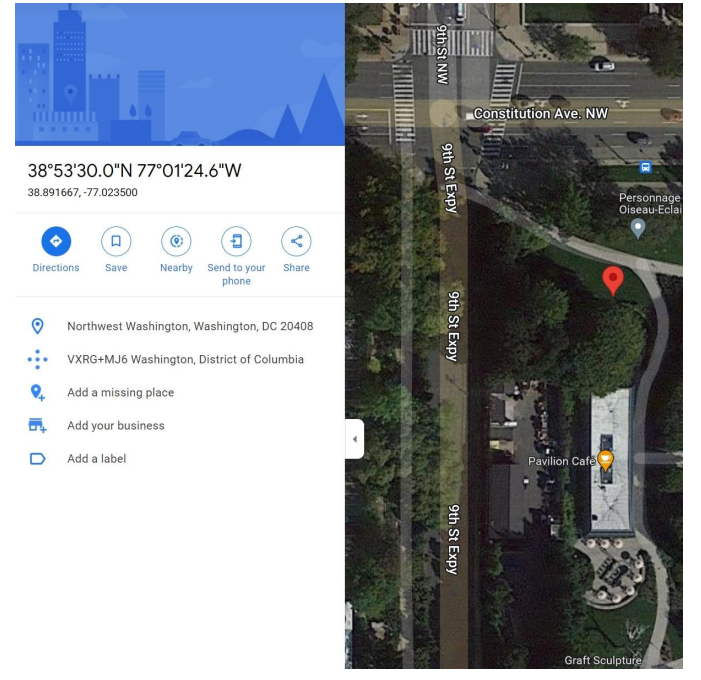
32		F: Carry T: Tracy	Carry almost arrives at the NGDC.	SMS Messages
33		F: Tracy T: Carry	Tracy tells Carry to meet her out front and that she will take the tablet in.	SMS Messages
34		F: Tracy T: Carry	Tracy asks about how Carry's flash mob is going.	SMS Messages
35		F: Terry T: Tracy	Terry messages Tracy about wanting to go to Joe's for the weekend and that he will take her to go shopping for school.	SMS Messages

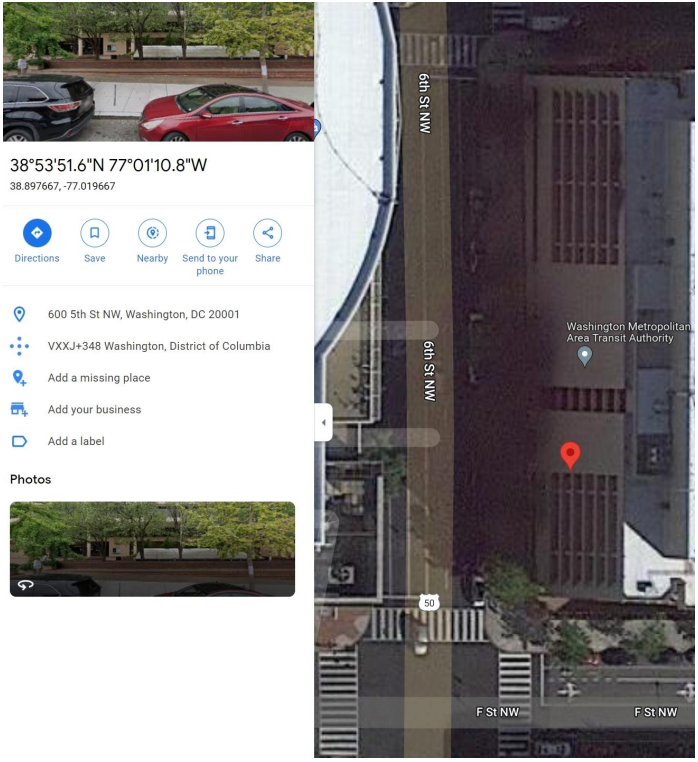
Appendix B: WiFi and GPS Location Information



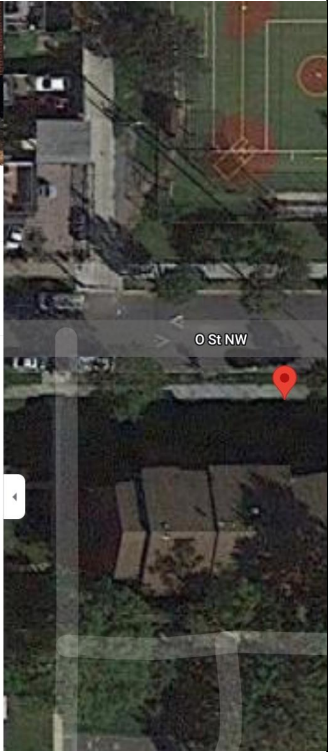
Location Information				
Artifact #	Timestamp	Header Information	Body	Map Screenshot
1	July 08, 2012 12:33:36 (CDT)	38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	
2	July 08, 2012 12:34:31 (CDT)	38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	
3	July 08, 2012 12:34:50 (CDT)	38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	

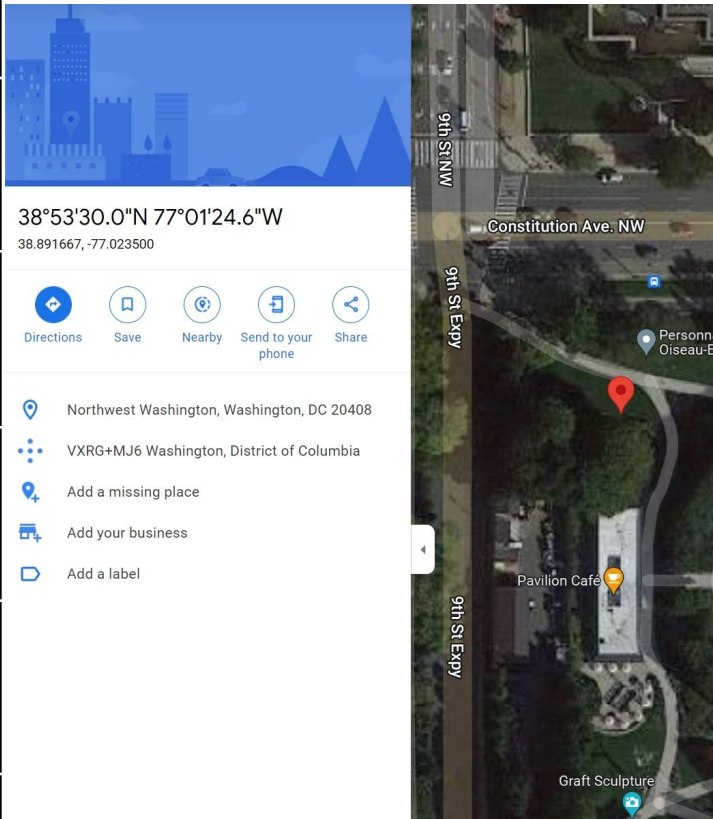
4	July 08, 2012 12:35:50 (CDT)	38°53'28.8"N 77°01'22.2"W	7th St NW, Washington, DC 20408	
5	July 08, 2012 12:36:30 (CDT)	38°53'28.8"N 77°01'21.0"W	Northwest Washington, Washington, DC 20408	

6	July 08, 2012 12:37:16 (CDT)	38°53'27.0"N 77°01'19.8"W	Northwest Washington, Washington, DC 20408	 <p>38°53'27.0"N 77°01'19.8"W 38.890833, -77.022167</p> <p>Directions Save Nearby Send to your phone Share</p> <p>Northwest Washington, Washington, DC 20408 VXRH+84P Washington, District of Columbia</p> <p>Add a missing place Add your business Add a label</p> <p>National Gallery of Art – Sculpture Garden Outdoor ice skating rink with a cafe Moondog Sculpture Madison Dr NW</p>
7	July 08, 2012 12:37:37 (CDT)	38°53'27.0"N 77°01'19.8"W	Northwest Washington, Washington, DC 20408	

8	July 08, 2012 12:41:41 (CDT)	38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	 <p>38°53'30.0"N 77°01'24.6"W 38.891667, -77.023500</p> <p>Directions Save Nearby Send to your phone Share</p> <p>Northwest Washington, Washington, DC 20408 VXRG+MJ6 Washington, District of Columbia</p> <p>Add a missing place Add your business Add a label</p> <p>Constitution Ave. NW Personnage Oiseau-Eclair Pavilion Cafe Graft Sculpture 9th St NW 9th St Expwy 9th St Expwy</p>
9	July 08, 2012 12:41:53 (CDT)	38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	
10	July 08, 2012 12:42:03 (CDT)	38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	

11	July 08, 2012 12:49:25 (CDT)	38°53'51.6"N 77°01'10.8"W	600 5th St NW, Washington, DC 20001	
12	July 08, 2012 12:49:37 (CDT)	38°53'51.6"N 77°01'10.8"W	600 5th St NW, Washington, DC 20001	
13	July 08, 2012 12:49:49 (CDT)	38°53'51.6"N 77°01'10.8"W	600 5th St NW, Washington, DC 20001	
14	July 08, 2012 12:50:07 (CDT)	38°53'51.6"N 77°01'10.8"W	600 5th St NW, Washington, DC 20001	
15	July 08, 2012 12:50:20 (CDT)	38°53'51.6"N 77°01'10.8"W	600 5th St NW, Washington, DC 20001	

16	July 08, 2012 12:51:44 (CDT)	38°54'30.6"N 77°01'05.4"W	1321 5th St NW, Washington, DC 20001	<div><p>38°54'30.6"N 77°01'05.4"W 38.908500, -77.018167</p><div><div>Directions</div><div>Save</div><div>Nearby</div><div>Send to your phone</div><div>Share</div></div><div><div><div>1321 5th St NW, Washington, DC 20001</div><div>WX5J+CP4 Washington, District of Columbia</div><div>Add a missing place</div><div>Add your business</div><div>Add a label</div></div><div><div>Photos</div><div><div>93+ Photos</div></div></div></div><div><p>O St NW</p></div></div>
----	---------------------------------------	------------------------------	--	---

17	July 08, 2012 12:59:55 (CDT)	38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	
18	July 08, 2012 01:00:01 (CDT)	38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	
19	July 08, 2012 01:00:07 (CDT)	38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	
20	July 08, 2012 01:00:12 (CDT)	38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	
21	July 08, 2012 01:00:23 (CDT)	38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	
22	July 08, 2012 01:02:23 (CDT)	38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	